

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK**

UNITED STATES OF AMERICA ,

v.

1:18-cr-326

TYLER KING,

Defendant.

**THOMAS J. McAVOY,
Senior United States District Judge**

DECISION & ORDER

I. INTRODUCTION

Defendant Tyler King is charged in the Superseding Indictment with one count of Conspiracy to Commit Computer Fraud in violation of 18 U.S.C. § 371, one count of Computer Intrusion Causing Damage in violation of 18 U.S.C. § 1030(a)(5)(A), and two counts of Aggravated Identity Theft in violation of 18 U.S.C. § 1028A. Sup. Ind., Dkt. No. 34. King moves (1) to suppress evidence obtained from electronic devices seized pursuant to a search warrant executed at his residence on August 25, 2016 (the “Electronic Evidence Motion”); (2) to suppress his August 25, 2016 statements to law enforcement pursuant to *Miranda v. Arizona*, 384 U.S. 436 (1966) (the “*Miranda* Motion”); and (3) for discovery and a bill of particulars (the “Discovery Motion”). Dkt. No. 29. The government opposes each motion. See Dkt. No. 32. The government also moves for a ruling that evidence of King’s November 2004 admission to FBI agents that he hacked into his high school’s

computer network (the “2004 Hack”) is admissible under Federal Rules of Evidence 401, 403, and 404(b). Dkt. No. 46. King opposes this motion. Dkt. No. 54.

II. DISCUSSION

a. Electronic Evidence Motion

1. Background

This case arises from the government’s belief that King conspired with Ashley St. Andria to gain unauthorized access to the computer network of an East Greenbush, New York-based technology company, referred to in the Superseding Indictment as Company A. *See generally*, Sup. Indict.¹ The alleged object of the conspiracy was to gain unauthorized access, and exceed authorized access, to Company A’s computer network so that King and St. Andria could read emails of Company A employees, view Company A’s personnel records, create new user accounts for Company A’s computer network, and modify Company A’s computer records. *Id.* ¶ 3. It is alleged that King and St. Andria accessed, without authorization, user accounts, used those user accounts to create new, unauthorized user accounts, and then used those unauthorized user accounts to access the emails of employees of Company A, view Company A’s personnel records, and modify Company A’s computer records. *Id.* ¶ 4. It is further alleged that King and St. Andria installed onto Company A’s computer network malicious software designed to capture network data, circumvent network passwords, and monitor network activities. *Id.* ¶ 5. The Superseding Indictment alleges that King directed St. Andria over the telephone in the commission of an

¹Ms. St. Andria was not charged in this case and is subject of a separate proceeding in this District in which she has entered a guilty plea to an indictment charging her with computer fraud in violation of 18 U.S.C. § 1030(a)(5)(A). *See* Plea Agreement, *United States v. St. Andria*, No. 1:17-CR-372 (TJM) (N.D.N.Y. Aug. 15, 2018), Dkt. No. 23.

overt act in furtherance of the conspiracy. *Id.* ¶ 6(a). It is also alleged that as a result of this conduct, King intentionally caused damage to a protected computer resulting in a loss during a one-year period in the aggregate of at least \$5,000 in value. *Id.* ¶ 2. Further, King is alleged that have knowingly caused the transmission of an unauthorized program, information, code, or command that caused damage to Company A's computer, and twice knowingly transferred, possessed, and used, without lawful authority, computer user names and computer passwords during and in relation to the alleged felony offense of accessing a protected computer and causing damage. See Sup. Indict., ¶¶ 7-9. It is believed that King and St. Andria accessed Company A's network remotely from their residences in Texas, and communicated with each other by cellular telephone to accomplish this scheme. See *generally*, FBI Special Agent Jeffrey A. Barrette's Affidavit in Support of Search Warrant, Dkt. No. 29-1, at 9-41.

2. Search & Seizure Warrant

On August 24, 2016, based on Special Agent Barrette's affidavit, the Hon. David L. Horan, U.S. Magistrate Judge of the U.S. District Court for the Northern District of Texas, issued a warrant authorizing federal officers to search King's residence at 3032 Larreta, Grand Prairie, TX 75054, and to seize property identified in Attachment B to the search warrant. See Dkt. No. 29-1, at 2-8. The warrant indicates:

Affidavit(s) having been made before me by FBI Special Agent Jeffrey A. Barrette has [*sic*] reason to believe that on the person of or on the property or premises known as 3032 Larreta, Grand Prairie, TX 75054, a residence further described in Attachment A . . . there is now concealed a certain person or property, namely [s]ee Attachment B. I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this

warrant. YOU ARE HEREBY COMMANDED to search on or before 8/31/16 the person or place named above for the person or property specified, serving this warrant and making the search (in the daytime - 6:00 A.M. to 10:00 P.M.) and if the person or property be found there to seize same, leaving copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to DAVID L. HORAN, United States Magistrate Judge as required by law.

Dkt. No. 29-1, at 2.

Attachment B lists the "Property to be Seized" as "[a]ll records and information relating to violations of 18 U.S.C. §§² 1030 (Unauthorized Access to a Protected Computer) involving Ashley ST. ANDRIA or Tyler KING, and occurring in 2015 and 2016, as set out in the Affidavit, including but not limited to the following: 1. Books, records, receipts, notes, ledgers, invoices or other papers or documents relating to [Company A], access of the [Company A] computer network, the use of the 'Hide.me' service, the use of online anonymizing services and/or proxy services, and the use of malicious software (e.g., software designed to monitor a computer without authorization; access a computer without authorization; capture data on a computer system without authorization; and circumvent passwords on a network); . . . 5. Computers and storage medium (as defined below);" *id.* at 5, and

6. For any computer or storage medium whose seizure is authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant

²Attachment B has two paragraph signs.

messaging logs, photographs, and correspondence; b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software; c. evidence of the lack of such malicious software; d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user; e. evidence indicating the computer user's state of mind as it relates to the crime under investigation; f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence; g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER; h. evidence of the times the COMPUTER was used; i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER; j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER; k. records of or information about Internet Protocol addresses used by the COMPUTER; l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; m. contextual information necessary to understand the evidence described in this attachment.

Id., at 6-7.

Attachment B provides that "the terms 'records' and 'information' includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies). *Id.*, at 7-8. It also provides that the term "computer" includes "all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical,

arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.” *Id.*, at 8. In addition, Attachment B provides that the term "storage medium" includes “any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CDROMs, and other magnetic or optical media.” *Id.* Finally as relevant here, Attachment B provides that if King’s iPhone 6 phone is found at the premises to be searched, law enforcement personnel are authorized to depress King’s fingerprint and/or thumbprint onto the sensor pad of the phone during the execution of the warrant. *Id.* at 8.

3. Fourth Amendment Particularity Requirement

King moves to suppress all evidence recovered as a result of the search of the electronic devices found at 3032 Larreta, Grand Prairie, TX, on the ground that “the warrant does not particularly authorize the search of these devices.” Def. Mem. L., at 3. He argues that the face of the warrant describes “what is to be searched: the physical premises of 3032 Larreta, Grand Prairie, TX 75054,” and that “the face of the warrant and Attachment B describe the items to be seized during the search: generally, items evidencing violations of Computer Fraud statutes,” but that the warrant “quite clearly does not . . . authorize the search of [the seized] devices.” *Id.* at 4.

Under the Fourth Amendment to the United States Constitution, “no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. To guard against indiscriminate searches and seizures, “the Fourth Amendment provides that ‘a warrant may not be issued unless probable cause is properly

established and the scope of the authorized search is set out with particularity.” *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Kentucky v. King*, 563 U.S. 452, 459 (2011)). The particularity requirement “guards against general searches that leave to the unguided discretion of the officers executing the warrant the decision as to what items may be seized.” *United States v. Riley*, 906 F.2d 841, 844 (2d Cir. 1990). “To be sufficiently particular under the Fourth Amendment, a warrant must satisfy three requirements,” —that is, it must: (1) “identify the specific offense for which the police have established probable cause”; (2) “describe the place to be searched”; and (3) “specify the items to be seized by their relation to designated crimes.” *United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017) (internal quotation marks omitted). The Second Circuit has observed that the nature of the search of electronic evidence “demands a heightened sensitivity to the particularity requirement.” *Galpin*, 720 F.3d at 447 (internal quotations and citation omitted).

King argues that “[t]he electronic devices enumerated in Attachment B are . . . items to be seized in the search, much like they might be if they were, say, stolen property stashed in the warehouse of a thief. The warrant quite clearly does not, however, authorize the search of these devices.” Def. Mem. L. at 4 (emphases in original). This argument, however, ignores Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, which applies to warrants seeking electronically stored information. The rule states that:

A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. *Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant.*

Fed. R. Crim. P. 41(e)(2)(B) (emphasis added). The Advisory Committee Note to Rule 41 further explains:

Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.

Fed. R. Crim. P. 41, Advisory Committee Note to Subdivision (e)(2), 2009 Amendments.

Under Rule 41(e)(2)(B), “a warrant for computer data presumptively ‘authorizes a later review of the media or information consistent with the warrant.’” *United States v. Ganius*, 824 F.3d 199, 231 (2d Cir. 2016)(quoting Fed. R. Crim. P. 41(e)(2)(B)).

Because the warrant attaches and incorporates Attachment B authorizing the seizure of computers and electronic devices found at King’s residence that may contain evidence of § 1030 violations, *see, e.g., Groh v. Ramirez*, 540 U.S. 551, 557–58 (2004) (explaining that courts may construe warrants with reference to supporting documents that are attached to the warrant and incorporated by reference), yet does not “otherwise specif[y]” that a later review of media or information on these devices is prohibited, the warrant authorizes a later review of the seized computer and electronic media for evidence of § 1030 violations under Rule 41(e)(2)(B). *See, e.g., United States v. Beal*, 730 F. App’x 30, 33 (2d Cir. 2018) (“[B]y expressly authorizing the search of [a particular place] and the seizure of electronic devices evidencing violations of 18 U.S.C. § 2252A, the warrant authorized the search of those items for evidence.”)(citing Fed. R. Crim. P. 41(e)(2)(B)). To accept King’s argument that the computers and electronic media could be seized but not later searched would render Rule 41(e)(2)(B) superfluous, a statutory interpretation that should be avoided. *See State Street Bank & Trust Co. v. Salovaara*, 326 F.3d 130, 139 (2d Cir. 2003) (“It is well-settled that courts should avoid statutory interpretations that render provisions superfluous . . .”).

Viewing the face of the warrant which incorporates and attaches Attachment B,³ the seizure and later search of the computers and digital media found at King's residence for evidence of § 1030 violations does not violate the particularity requirement of the Fourth Amendment. See, e.g., Fed. R. Crim. P. 41(e)(2)(B); *Beal*, 730 F. App'x at 32-33; see also *United States v. Fifer*, 863 F.3d 759, 766 (7th Cir. 2017)(affirming denial of motion to suppress evidence obtained from defendant's cellular phones and tablet device found in his residence premised on argument that subject warrant only authorized search of defendant's residence and seizure of his electronic devices, because it "makes more sense to read a search warrant's command to seize an electronic device as including a concomitant directive to search that device's digital contents"); *United States v. Reed*, No. 2:13-cr-29-1, 2013 WL 5503691, at *4- 5 (D. Vt. Oct. 2, 2013) (rejecting defendant's argument that subject warrant "authorized law enforcement to seize, but not search, the cell phones found at his residence" premised on claim that his cellular phone was not listed in Attachment A to the subject warrant).

4. Plain View Doctrine

King also argues that "[o]n information and belief, . . . there was nothing in plain view that agents would have noted during the authorized search of the physical premises that would have indicated the computers were tied to the crimes being investigated to be searched at a later date." Def. Mem. L., at 5. However, given the nature of the underlying crime, invocation of the plain view doctrine is unfounded. "The plain view doctrine permits

³The Court does not consider the supporting affidavit in its consideration of the search warrant because the warrant did not "use[] appropriate words of incorporation" and the affidavit was not attached to the warrant. *United States v. Waker*, 534 F.3d 168, 172 (2d Cir. 2008) (citing *Groh*, 540 U.S. at 557).

an officer to seize evidence *outside a warrant's authorization* when it is immediately apparent that the object is connected with criminal activity, and where such search and seizure do not involve an invasion of privacy.” *Galpin*, 720 F.3d at 451 (internal quotations and citation omitted) (emphasis added). Here, the warrant authorized the seizure of computers and electronic media evidencing violations of § 1030 related to unauthorized access to a protected computer. In order to determine if the seized items evidenced such violations, the warrant necessarily authorizes a later review of the media or information of the seized computers and electronic media. See Fed. R. Crim. P. 41(e)(2)(B); *see also In the Matter of a Warrant for All Content and Other Info. Associated with the Email Account xxxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc.*, 33 F. Supp. 3d 386, 392 (S.D.N.Y. 2014), as amended (Aug. 7, 2014) (“In the context of suppression motions, courts have routinely upheld the seizure or copying of hard drives and other storage devices in order to effectuate a proper search for the categories of documents or files listed in a warrant.”)(citing cases).

5. Separate Search Warrant

King also argues that the government should have obtained a separate search warrant for the electronic devices as King believes the government did for St. Andria’s personal cellular phone. See Def. Mem. L., at 5 (“on information and belief,” the government obtained an August 24, 2016 warrant in this District for St. Andria’s personal cellular phone). The government asserts that no such warrant was ever sought “as it was not necessary for the same reasons that the warrant to search the defendant’s residence authorized seizure of electronic evidence found on devices located therein.” Gov. Mem. L.,

at 9, n. 1. For the reasons discussed above, no separate search warrant was necessary to search the computers and electronic devices seized at King's residence on August 25, 2016 for evidence of § 1030 violations. Thus, the motion on this ground is denied.

6. Fruit of the Poisonous Tree Doctrine

There is also no merit to King's argument that the Court should suppress his statements to law enforcement during the search of his residence as fruit of the poisonous tree. See Def. Mem. L., at 5. First, because the warrant is valid, "there is no poisonous tree," so "there is no fruit to suppress." *United States v. Lustyik*, 57 F. Supp. 3d 213, 233 (S.D.N.Y. 2014) (denying motion to suppress defendant's statements made to law enforcement during search of his residence pursuant to valid warrant). Second, because the agents were lawfully in King's residence during the interview, there is no basis to find that King's statements to them are somehow the fruits of an unlawful search that should be suppressed. See *Lustyik*, 57 F. Supp. 3d at 233.

7. Good Faith Exception

Even if the search of King's computers and electronic devices amounted to a Fourth Amendment violation, suppression would not be warranted here. A determination that a Fourth Amendment violation occurred "does not automatically require the suppression of all physical evidence seized or statements derived from that illegal search." *United States v. Bershchansky*, 788 F.3d 102, 112 (2d Cir. 2015). In *United States v. Leon*, the Supreme Court set out an exception to the exclusionary rule for a search conducted in "reasonable, good-faith reliance on a search warrant that is subsequently held to be defective." 468 U.S. 897, 905 (1984). In determining whether to apply the good faith exception, courts examine

“whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances.” *United States v. Rosa*, 626 F.3d 56, 64 (2d. Cir. 2010) (internal quotations and citations omitted). “To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.” *Herring v. United States*, 555 U.S. 135, 144 (2009). Further, “suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule.” *Leon*, 468 U.S. at 918.

Suppression is not warranted where agents rely in good faith on a search warrant that lacks particularity and “their actions bear none of the hallmarks of a general search.” *Rosa*, 626 F.3d at 66 (refusing to suppress based on executing agent’s good faith reliance on defective warrant); see *United States v. Clark*, 638 F.3d 89, 99 (2d Cir. 2011) (recognizing “an exception to the exclusionary rule for evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant”)(internal quotation marks omitted); see also *Davis v. U.S.*, 564 U.S. 229, 238 (2011)(“[W]hen the police act with an objectively ‘reasonable good-faith belief’ that their conduct is lawful . . . the deterrence rationale loses much of its force, and exclusion cannot pay its way.”)(internal quotations and citations omitted)). “Thus, the good-faith inquiry here ‘is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances.’” *Bershchansky*, 788 F.3d at 113 (quoting *Herring v. United States*, 555 U.S. 135, 145 (2009)).

“While [courts] may no longer rely on unincorporated, unattached supporting documents to cure a constitutionally defective warrant, those documents are still relevant to our determination of whether the officers acted in good faith, because they contribute to our assessment of the officers' conduct in a particular case.” *Rosa*, 626 F.3d at 64. “Unless there is evidence that law enforcement officers ‘actually relied on the defective warrant, as opposed to their knowledge of the investigation and the contemplated limits of the [issuing magistrate]’s authorization, in executing the search, the requisite levels of deliberateness and culpability justifying suppression are lacking.” *Lustyik*, 57 F. Supp. 3d 227 (quoting *Rosa*, 626 F.3d at 66). Here, based upon Rule 41(e)(2)(B), the language of Attachment B, and the allegations in Special Agent Barrette’s affidavit in support of the warrant, it was objectively reasonable for law enforcement officials to construe the warrant to authorize the seizure and later search of King’s computers and electronic devices for evidence of § 1030 violations. In light of all the circumstances, a reasonably well-trained officer executing the warrant would not have known that the search of these devices exceeded the scope of the warrant, and therefore, suppression would serve no deterrent purpose and is unwarranted. See *Davis*, 564 U.S. at 237 (“For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs.”); *Beal*, 730 F. App’x at 33 (“We also agree with the district court that even if the warrant were invalid, the good faith exception to the exclusionary rule applies because the officers’ reliance upon the warrant was objectively reasonable. As the warrant was not facially deficient, for the reasons set forth above, we agree that a reasonably well-trained officer executing the warrant would not have known that the search and seizure exceeded the scope of the warrant, and therefore, suppression

would serve no deterrent purpose and is unwarranted.”)(internal quotation marks and citations omitted); *United States v. Miller*, No. 13-CR-6036L, 2013 WL 4505458, at *5 (W.D.N.Y. Aug. 16, 2013) (“In this case, I find that even if it could be said that the officers exceeded the textual scope of the Search Warrant, it was objectively reasonable for them to construe the warrant to authorize the search of the digital camera and memory card. Accordingly, I recommend that Miller's motion also be denied under the *Leon* good-faith exception.”).

b. *Miranda* Motion

King argues that during execution of the search warrant he was subjected to custodial interrogation without being advised of his *Miranda* rights. The government concedes that King was interrogated but argues that *Miranda* warnings were not required because King was not in custody. See Gov. Mem. L. at 11 (“No *Miranda* warnings were required . . . because the defendant—although interrogated—was never in custody.”) King also contends that during his interrogation, he was twice denied the right to consult with an attorney, and that because of the coercive nature of the encounter, his statements were not voluntary. The Court conducted an evidentiary hearing on October 29, 2019 to resolve these issues.

1. Custody

Normally, custody is established if, in light of the circumstances of an interrogation, a reasonable person in the suspect's position would have felt that he was not at liberty to terminate the interrogation and leave. *Yarborough v. Alvarado*, 541 U.S. 652, 63 (2004); see *United States v. Familetti*, 878 F.3d 53, 60 (2d Cir. 2017) (“In evaluating whether the

degree of a restraint is custodial, we look to whether a reasonable person in the suspect's shoes would not have felt free to leave under the circumstances.”)(internal quotation marks and citation omitted). “The test for determining custody is an objective inquiry that asks (1) ‘whether a reasonable person would have thought he was free to leave the police encounter at issue’ and (2) whether ‘a reasonable person would have understood his freedom of action to have been curtailed to a degree associated with formal arrest.’” *United States v. Faux*, 828 F.3d 130, 133 (2d Cir. 2016)(citing *United States v. Newton*, 369 F.3d 659, 672 (2d Cir. 2004)). “Although both elements are required, the second is the ‘ultimate inquiry’ because a ‘free-to-leave inquiry reveals only whether the person questioned was seized.’” *Id.* (quoting *Newton*, 369 F.3d at 672 (internal quotation omitted)).

An individual who understands that [his] detention is “not likely to be temporary and brief” and feels that [he] is “completely at the mercy of police” could reasonably deem [his] situation comparable to formal arrest. *Newton*, 369 F.3d at 675 (quoting [*Berkemer v. McCarty*, 468 U.S. 420, 437–38 (1984)]). Relevant considerations include: (1) “the interrogation's duration”; (2) “its location (e.g., at the suspect's home, in public, in a police station, or at the border)”; (3) “whether the suspect volunteered for the interview”; (4) “whether the officers used restraints”; (5) “whether weapons were present and especially whether they were drawn”; and (6) “whether officers told the suspect he was free to leave or under suspicion.” [*United States v. FNU LNU*, 653 F.3d 144, 153 (2d Cir. 2011)](internal citations and alterations omitted).

Id.

Here, the credible evidence establishes that on August 25, 2016 at 6:00 AM, 18 FBI agents and 2 local police officers arrived at King's residence to execute the above-referenced search warrant. See Gov. Ex. 1. Some of these law enforcement officers knocked on King's front door and announced their presence. King was awakened by the officers' loud knocking and first approached the door with a handgun. When he observed

the flashing lights from a police cruiser, King concluded that it was law enforcement at the door and therefore returned his handgun to his bedroom, placing it on the bed. King then answered the door dressed only in his underwear. When King opened the door he saw three FBI agents with assault rifles pointed at him, with one behind a protective shield. The officers at the door were members of the entry team tasked with entering and sweeping the residence to ensure that no threats existed. Prior to approaching King's residence, FBI agents became aware that King had a federal firearms license and therefore were concerned for the safety of themselves and others. The officers at the door instructed King to turn around so they could place him in handcuffs. King complied and advised the officers that he had placed his handgun on the bed in his bedroom.⁴ King was then escorted to a secure location outside the residence where he remained for approximately 30 minutes while the entry team secured the residence. King's wife was also in the residence at the time, and she too was escorted to the secure location where King was brought. She was never placed in handcuffs. FBI Special Agent Jeffrey Barrette was at the secure location and stood with King while the entry team swept the residence. Special Agent Barrette did not have his weapon drawn at the time nor did he draw it at any time on August 25, 2016. King was not questioned while he was at the secure location.

After the entry team indicated that the residence was secure, Special Agent Barrette and Special Agent Sharon McLaughlin accompanied King into the residence and into a

⁴This handgun was later found and secured by the entry team, as were other weapons found in a safe in the residence.

room on the first floor.⁵ King's handcuffs were removed. The agents identified themselves, showed King their credentials, explained that they were executing a search warrant in connection with their investigation into a computer intrusion crime at Company A (using the name of the company), told King that he was not under arrest and that he was free to leave, and asked whether he would be willing to speak to the agents. King agreed to do so. The agents sat on chairs facing King, who also sat on a chair. King appeared to the agents to understand that he was not under arrest and was free to leave, and that he freely agreed to speak to them. While in the room, law enforcement officers brought clothes for King to put on over his underwear. The agents retrieved the clothes because they did not want third parties walking into the secure locations while the search warrant was being executed. The agents perceived King as calm and confident. At no time during the encounter on August 25, 2016 did King indicate that he wanted an attorney present or ask whether he needed one.

Special Agent Barrette asked King questions while Special Agent McLaughlin took notes. King gave expansive answers to Special Agent Barrette's questions but refused the request to provide passwords for his computers. Shortly after the interview began, King asked if his wife could be present, to which the agents agreed. King's wife came into the room and sat on a piano bench. Like with King, the agents identified themselves, advised King's wife that they were there to execute a search warrant, and explained that she was not under arrest and was free to leave.

After approximately an hour, Special Agent Barrette was called to another place in

⁵Pictures of the room show that there was a drum set and an electronic piano in the room, along with three wooden chairs and a bench for the electronic piano. Gov. Ex. 7.

the residence to answer questions from agents executing the search warrant. Special Agent McLaughlin was still in the room with King but she did not ask him any questions or interview him at this time. King asked to leave the room, apparently to go to some other location in the residence. Special Agent McLaughlin advised King that if he wanted to leave the room to go to another part of the residence he would need to be accompanied by an agent because the residence was secure and agents were in the process of executing the search warrant. Despite being told this, King left the room unaccompanied and began walking away from the front door and into the interior of the residence. Special Agent McLaughlin followed but King immediately encountered another agent who told King he could not go unaccompanied into secured locations in the residence. King returned to the room where the interview had been conducted and waited for Special Agent Barrette's return.

When Special Agent Barrette returned, he resumed the interview. At this point, King indicated that he did not want to talk anymore and that he wanted to leave. The interview ceased and the agents arranged to have one of King's vehicles cleared so he and his wife could leave in it. The agents told King that the execution of the search warrant would continue in his absence. King told the agents to leave the door unlocked but to activate the security alarm. Special Agent Barrette also asked King whether there was someone he could call to notify them when the search warrant execution was finished, and King gave him his father's telephone number who Special Agent Barrette called when they were finished. At 7:53 AM, King and his wife left the premises in their vehicle. See Gov. Ex. 1, at 2.

In light of the facts established at the evidentiary hearing, a reasonable person under

similar circumstances would have thought he was free to leave the police encounter at issue and, thus, would not have understood his freedom of action curtailed to a degree associated with formal arrest. Although King was initially detained at gunpoint, handcuffed, and removed to a location outside of his residence, this detention was temporary and lasted for approximately 30 minutes. King was not questioned during this period, he was returned to his residence, and his handcuffs were removed. The fact that King was initially detained at gun point and handcuffed does not render the subsequent interrogation custodial. See *Familetti*, 878 F.3d at 61 (a suspect's "initial restraints cannot establish a state of custody for the duration of his interactions with the police."); *United States v. Bershchansky*, 958 F. Supp. 2d 354, 383 (E.D.N.Y. 2013) ("Even the use of handcuffs prior to an interrogation, however, does not automatically render the interrogation custodial."), *aff'd*, 788 F.3d 102 (2d Cir. 2015); see also *United States v. Cota*, 953 F.2d 753, 758-59 (2d Cir. 1992) (defendant not in custody where the "initial use of guns and handcuffs [were] necessitated by the officer's safety, but the handcuffs were removed as soon as . . . the perceived safety threat abated"). In addition, King was told that he was not under arrest and that he was free to leave, which he appeared to understand. "Such advice, while not dispositive, is probative in assessing the extent to which a reasonable person would understand any restraints on his freedom." *Familetti*, 878 F.3d at 60 (internal citation and quotation marks omitted); see *Newton*, 369 F.3d at 676 (informing a suspect that he is not under arrest and is free to leave "is a fact that may be considered in assessing the extent to which a reasonable person would understand any restraints on his freedom to be comparable to those associated with a formal arrest").

King also agreed to speak with the agents, and provided expansive answers to

Special Agent Barrette's questions. While King's expansive answers to Special Agent Barrette's questions indicates that he freely agreed to be interviewed, he also refused to provide the passwords to his computers. This refusal indicates that King understood his right to decline to speak or provide any specific information requested by the officers. It is also significant that after being questioned for approximately one hour and after Special Agent Barrette left the room, King attempted to walk into a part of the residence where the search was being executed despite Special Agent McLaughlin telling him he could not do so. This hardly indicates that King believed he was under constraint similar to that of a formal arrest or that he was at the mercy of the law enforcement officers. Still further, after Special Agent Barrette returned to the room to recommence the interview, King decided to end the interview and leave the residence. This evinces King's awareness of his ability to refuse to speak to the agents and to leave the premises, thereby supporting the conclusion that a reasonable person under the same circumstances would not have believed that he was under the constraints of a formal arrest or at the mercy of law enforcement.

Furthermore, the interrogation was conducted entirely in King's home, a familiar surrounding which a reasonable person would not find to be a custodial detention similar to a formal arrest. See *Newton*, 369 F.3d at 675 ("[A]bsent an arrest, interrogation in the familiar surroundings of one's own home is generally not deemed custodial."); *United States v. Rakowski*, 714 F. Supp. 1324, 1334 (D. Vt. 1987) ("Lower courts . . . almost universally hold that questioning in a suspect's home is not custodial . . ."); accord *United States v. Konn*, 634 F. App'x 818, 821 (2d Cir. 2015) (no custody where agents searched defendant's home, told defendant he was not under arrest and free to leave). Also, King's wife was allowed to participate in the questioning, a fact that would indicate to a reasonable

person that the questioning was not conducted under constraints consistent with a formal arrest.

Under the totality of the circumstances as addressed above, a reasonable person would not have believed he was in custody during the period that King was questioned by federal agents. Thus, *Miranda* warnings were not required.

2. Request for Counsel

The credible evidence indicates that King made no statement to the agents that could reasonably be construed as a request for counsel during the interrogation. See *United States v. Oehne*, 698 F.3d 119, 122–23 (2d Cir. 2012) (“For a suspect to invoke his *Miranda* right to counsel, he must at a minimum make ‘some statement that can reasonably be construed to be an expression of a desire for the assistance of an attorney in dealing with custodial interrogation.’”)(quoting *McNeil v. Wisconsin*, 501 U.S. 171, 178 (1991)) (emphasis omitted). Thus, the agents were not required to cease their questioning during the interview. See *Edwards v. Arizona*, 451 U.S. 477, 484–85 (1981)(law enforcement officers must immediately cease questioning of a suspect who clearly asserts his right to have counsel present during custodial interrogation); *United States v. Gonzalez*, 764 F.3d 159, 165 (2d Cir. 2014)(Once a defendant invokes his right to counsel during a custodial interrogation, questioning must cease.); see also *Davis v. United States*, 512 U.S. 452, 459 (1994)(“We decline petitioner’s invitation to ... require law enforcement to cease questioning immediately upon the making of an ambiguous or equivocal reference to an attorney.”); *id.* at 61-62 (“[W]e decline to adopt a rule requiring officers to ask clarifying questions. If the suspect’s statement is not an unambiguous or unequivocal request for counsel, the officers have no obligation to stop questioning him.”); *Oehne*, 698 F.3d at 123 (“If an accused

makes a statement concerning the right to counsel that is ambiguous or equivocal or makes no statement, the police are not required to end the interrogation, or ask questions to clarify whether the accused wants to invoke his or her *Miranda* rights.”)(quoting *Berghuis v. Thompson*, 560 U.S. 370, 381 (2010)). Under these circumstances, no *Miranda* violation occurred.

3. Voluntariness

The government must prove voluntariness by a preponderance of the evidence. *United States v. McFarland*, 424 F. Supp. 2d 427, 434 (N.D.N.Y. 2006) (citing *Missouri v. Seibert*, 542 U.S. 600, at 610, n. 1 (2004)). Voluntariness is assessed under a “totality of the circumstances” approach. *United States v. Okwumabua*, 828 F.2d 950, 953 (2d Cir. 1987); see also *United States v. Ferrara*, 377 F.2d 16, 17 (2d Cir. 1967), *cert. denied*, 389 U.S. 908 (1967)(“The Supreme Court has consistently made clear that the test of voluntariness [of a confession] is whether an examination of all the circumstances discloses that the conduct of ‘law enforcement officials was such as to overbear (the defendant’s) will to resist and bring about confessions not freely self-determined”)(quoting *Rogers v. Richmond*, 365 U.S. 534, 544, 81 S. Ct. 735, 741, 5 L. Ed.2d 760 (1961)). Relevant factors include “the type and length of questioning, the defendant’s physical and mental capabilities, and the government’s method of interrogation.” *Okwumabua*, 828 F.2d at 952. “If a statement is made as the result of coercion or other improper inducement that overbears a defendant’s will, the statement is not voluntary.” *United States v. Bowen*, No. 18-CR-00205-2 (NSR), 2019 WL 2240258, at *6 (S.D.N.Y. May 23, 2019)(citing *United States v. Ortiz*, No. 06-CR-6076, 2007 WL 925731, at *7 (W.D.N.Y. Mar. 26, 2007) (in turn citing *Hayes v. State of Washington*, 373 U.S. 503, 513-14 (1963))).

Although law enforcement officers arrived *en mass* at King's residence at 6:00 AM, roused him from his bed, pointed weapons at him, and handcuffed him, the credible evidence indicates that King remained calm from the beginning. While the officers observed that King's wife appeared shaken, they did not observe this in King. Furthermore, King remained in handcuffs for only approximately 30 minutes, and then was returned to his residence where he was advised that he was free to leave, not required to speak to the officers, and asked whether he was willing to speak with the agents - to which he agreed. The interrogation occurred in a room in King's residence where he and the agents sat on chairs, King was not handcuffed, the officers did not have their weapons drawn, and King's wife was allowed to participate in the questioning. The evidence indicates that Special Agent Barrette asked King questions about the computer intrusion crime underlying the investigation, and King gave expansive answers in response. While Special Agent Barrette testified that his interview technique was to establish rapport with King to obtain information from him, there is no indication that Special Agent Barrette or any other officer made statements or took actions that could be interpreted as a form of coercion to answer questions or as improper inducement designed to overbear King's will. Furthermore, the facts indicate that King has a number of advanced degrees and certificates, including legal and paralegal degrees and certificates, business degrees and certificates, a certificate in professional investigations, and a bachelor of science degree in criminal justice. King has also worked as a military police officer in the Army Reserves, applied to be a police reservist in Dallas, and had received a conditional offer of employment to be an FBI special agent. All this education and training certainly allowed King to make a voluntary and intelligent decision whether to agree to speak with the agents, or to decline to do so and leave as the

agents told him he was entitled to do. Quite contrary to the contention that King was confused by what was occurring, Special Agent McLaughlin testified that King acted like he was smarter than anyone else.

Based on the totality of the circumstances, the government has met his burden of demonstrating that King voluntarily made his statements to the agents on August 25, 2016.

4. Conclusion as to *Miranda* Motion

For the reasons set forth above, King's *Miranda* Motion seeking to suppress his statements to law enforcement officers on August 25, 2016 is denied.

c. Discovery Motion

1. Bill of Particulars

King demands that the government "provide all instances in which it is alleged and will be alleged that [he] acted in a [c]onspiracy with St. Andria including specific dates and times and specific communications referenced in such allegations in the [d]iscovery provided given that there are over 6,000 pages of [d]iscovery provided to date." Def. Mem. L., at 9, Item I. Beyond suggesting that the 6,000 pages of discovery already provided by the government is voluminous, the defendant provides no support for what is apparently his demand for a bill of particulars.

Under Federal Rule of Criminal Procedure 7(f), a district court may require the government to file a bill of particulars when it is necessary to explain the nature of the charges against the defendant, to allow him to prepare for trial, and to prevent unfair surprise. *See United States v. Bortnovsky*, 820 F.2d 572, 574 (2d Cir. 1987)(*per curiam*). The decision to grant a request for a bill of particulars is within the Court's discretion. *Id.* "Courts are only required to grant a bill of particulars 'where the charges of the indictment

are so general that they do not advise the defendant of the specific acts of which he is accused.” *United States v. Raniere*, No. 18-CR-2041 (NGG/VMS), 2019 WL 1903365, at *25 (E.D.N.Y. Apr. 29, 2019)(quoting *United States v. Chen*, 378 F.3d 151, 163 (2d Cir. 2004) (citation and quotation marks omitted)). “This standard turns on whether the information sought is necessary, not whether it is helpful.” *Id.* (citation and quotation marks omitted). “In making this determination, ‘the court must examine the totality of the information [already] available to the defendant—through the indictment, affirmations, and general pre-trial discovery.’” *Id.* (quoting *United States v. Bin Laden*, 92 F. Supp. 2d 225, 233 (S.D.N.Y. 2000) and citing *Bortnovsky*, 820 F.2d at 574 (“Generally, if the information sought by [the] defendant is provided in the indictment or in some acceptable alternate form, no bill of particulars is required.”)).

A bill of particulars is not meant to serve as “a general investigative tool, a discovery device or a means to compel the government to disclose evidence or witnesses to be offered prior to trial.” *United States v. Gibson*, 175 F. Supp. 2d 532, 537 (S.D.N.Y. 2001); see *United States v. Kang*, No. 04-CR-87 (ILG), 2006 WL 208882, at *1 (E.D.N.Y. Jan. 25, 2006)(A bill of particulars is not meant to enable a defendant to “obtain a preview of ... the government’s evidence before trial,” or “to learn the legal theory upon which the government will proceed.”). The defendant bears the burden of showing that the information sought is necessary and that he will be prejudiced without it. *Raniere*, 2019 WL 1903365, at *25 (citation quotation marks omitted).

Defendant fails to satisfy his burden of demonstrating the necessity of a bill of particulars as requested, or that he will be prejudiced without it. The conspiracy count of the Superseding Indictment, Count 1, details, among other things: (1) the participants in the

alleged conspiracy; (2) the dates on which the alleged computer intrusions took place; (3) the way in which the defendant and his co-conspirator carried out their scheme; (4) the names of the programs that the defendant is alleged to have unlawfully installed on the subject company's computer network; and (5) the names of the user accounts allegedly compromised by the defendant and his co-conspirator. See *generally* Sup. Indict., Dkt. No. 34. Moreover, the government represents that the discovery in this case provides ample detail about the nature of the allegations against the defendant. According to the government, this discovery includes, among other things: (1) detailed agency reports about the investigation; (2) files from the company concerning the incident at the heart of the indictment; and (3) extensive records obtained from third parties pursuant to subpoenas.

In light of the details in the Superseding Indictment and the extensive discovery provided by the government, King fails to show that the information sought in the requested bill of particulars is necessary to his defense or that he will be prejudiced without it. Accordingly, the demand for a bill of particulars is denied.

2. Miscellaneous Discovery Demands

Next, King raises a litany of itemized discovery demands, which the Court addresses *seriatim*.

Item A. In Item A, the defendant seeks the search warrant for St. Andria's personal cellular phone. As indicated above, the government represents that no such warrant was ever sought. Accordingly, the motion in this regard is denied.

Item B. In Item B, the defendant seeks "an e-mail . . . sent to AUSA Myers on October 17, 2017 with a 'Summary Document' possibly created by FBI Agent Marc Smith." Def. Mem. L. at 8. The government contends that the referenced document would only be

discoverable pursuant to Fed. R. Crim. P. 26.2 and 18 U.S.C. § 3500 (together, the “Jencks Act”), and indicates that it will disclose any documents subject to disclosure under these sources of law (“Jencks Material”) 14 days prior to the start of trial as required by Paragraph II.E of the Pretrial Scheduling Order. The government further represents that to the extent it expects to call the document’s author during its case-in-chief, it will re-review this document and determine whether it must be produced as Jencks Material. This satisfies the government’s obligation, and the motion in this regard is denied subject to renewal at trial if necessary.

Item C. In Item C, defense counsel claims that he is unaware of why certain documents in the government’s production are slipsheets that state “Produced in Native Format.” The government responds that this is a typical practice, and that all files that state “Produced in Native Format” bear a Bates number. The government asserts that the same Bates number is assigned to a corresponding “native” file in a discrete, marked folder in the government’s production called “Native,” which includes files, including Excel spreadsheets, that were produced in their original file format instead of being imaged. Because the defendant received the discovery materials, the motion in this regard is denied.

Item D. In Item D, King requests that the government provide all Proffer Agreements, Cooperation Agreements, Plea Minutes, Grand Jury minutes and other recorded statements and testimony of co-conspirator St. Andria. The government recognizes that the referenced documents would be discoverable as Jencks Material and/or pursuant to *Giglio v. United States*, 405 U.S. 150 (1972) (“*Giglio*”), which are due 14 days prior to the start of trial pursuant to Paragraphs II.D-E of the Pretrial Scheduling Order. Further, the government represents that the documents will be made available to the

defense 14 days prior to trial to the extent the government expects to call St. Andria during its case-in-chief. This satisfies the government's obligation, and the motion in this regard is denied subject to renewal at trial if necessary.

Item E. In Item E, King seeks St. Andria's personnel file(s) gathered from former employers including the victim-company in the Indictment. The government represents that it is in possession of certain documents received from the victim-company related to St. Andria's employment. It indicates that to the extent any of these documents are Jencks Material or fall within the scope of *Giglio*, the government will disclose any such document to the defendant 14 days before trial. This satisfies the government's obligation, and the motion in this regard is denied subject to renewal at trial if necessary.

Item F. In Item F, King requests the Court to issue an order directing the Government to provide him "with all types of *Brady*, Jencks and *Giglio* material at least two (2) weeks prior to trial so as to allow Defendant adequate preparation time and avoid senseless delay during trial." Def. Mem. L. at 8. The government responds that pursuant to Paragraph II.B.2 of the Pretrial Scheduling Order, it informed defense counsel on March 1, 2019 that it was unaware of any evidence favorable to the defendant on the issues of guilt or punishment within the scope of *Brady*, and that this is still the case. The government further represents that, as ordered by the Pretrial Scheduling Order, it will disclose 14 days before trial all Jencks Material and, to the extent it exists, any information in the government's possession that is within the scope of *Giglio*. This satisfies the government's obligation, and the motion in this regard is denied subject to renewal at trial if necessary.

Item G. In Item G, King requests that the government provide any other of his written, recorded or oral statements other than those referred to in the FBI FD-302 which he

attaches to his motion. The government responds that it has produced all of the defendant's written or recorded statements in its possession within the scope of Fed. R. Crim. P. 16(a)(1)(B), as it informed the defendant on March 1, 2019. This satisfies the government's obligation, and the motion in this regard is denied.

Item H. In Item H, King requests that the Court order the government to provide him expert witness reports at least 2 weeks prior to trial. The government responds that it previously disclosed Roderick Link as an expert and produced to the defendant on March 1, 2019 Mr. Link's report. This satisfies the government's obligation, and the motion in this regard is denied.

Item I. In Item I, King makes his request for a bill of particulars. For the reasons discussed above, the motion in this regard is denied.

Item J. In Item J, King requests "any witness statements in possession of the Government or its agents including but not limited to any statement of Jennifer King or statements by any other witness whether the Government intends to call them as a witness or not." Def. Mem. L. at 9. The government argues that all "witness statements" in the government's possession are not discoverable, and indicates that to the extent not already produced, it will disclose all relevant prior statements of its witnesses within its possession 14 days prior to the start of trial as Jencks Material. This satisfies the government's obligation, and the motion in this regard is denied subject to renewal at trial if necessary.

d. Government's Motion In Limine

The government moves for a ruling that evidence of King's November 2004 admission to FBI agents that he hacked into his high school's computer network (the "2004 Hack") is admissible under Federal Rules of Evidence 401, 403, and 404(b). The

government asserts that the evidence is offered for identification purposes and to demonstrate that the defendant had the technical ability, and thus the opportunity, to accomplish the hacks subject of this proceeding. King opposes the motion on various grounds arguing, principally, that even if relevant the evidence is prohibited propensity evidence under Rule 404(b)(1).

The Second Circuit has adopted an inclusionary approach to other act evidence under Rule 404(b), allowing such evidence to be admitted for any purpose provided it does not demonstrate criminal propensity. *United States v. Scott*, 677 F.3d 72, 79 (2d Cir. 2012). The Circuit has emphasized that this inclusionary rule “is not a carte blanche to admit prejudicial extrinsic act evidence when ... it is offered to prove propensity.” *Id.* Rather, for other act evidence to be admissible, it must: (1) be offered for a proper purpose, (2) be relevant to a material issue in dispute, (3) hold probative value substantially outweighing its potential for unfair prejudice under Rule 403, and (4) be accompanied by an appropriate limiting instruction to the jury. *United States v. Curley*, 639 F.3d 50, 56-57 (2d Cir. 2011); see *United States v. LaFlam*, 369 F.3d 153, 156 (2d Cir. 2004).

1. “offered for a proper purpose”

The government asserts that the 2004 Hack bears striking resemblance to the hacking activity in this case, see Gov’t Pretrial Br. (Dkt. No. 43) at 1-2,⁶ in that King hacked

⁶In the instant case, the government alleges that in September 2015, the defendant helped St. Andria create fraudulent administrator accounts on Company A’s computer network in New York. See Gov’t Pretrial Br. (Dkt. No. 43) at 1-2. The defendant and St. Andria allegedly created the fraudulent administrator accounts so they could, among other things, delete computer logs showing that St. Andria had previously accessed the accounts of other Company A employees (which she allegedly accomplished by using a standard password used for new employee accounts) to view their emails. *Id.* at 2. The defendant and St. Andria then purportedly used those accounts, and others, to review Company A’s business records and view the emails of other Company A employees. *Id.* After several weeks, Company A identified the fraudulent accounts and traced their creation to St. Andria’s network activity. *Id.* After Company A fired St. Andria in

(continued...)

into the high school computer, created two administrator accounts and attempted to disguise one of the accounts by making it consistent with the school's default naming convention for user accounts (keyed to each student's initials and identification number), and admitted that he considered "installing a password cracking program" on the network but never followed through. The government anticipates that King will argue at trial that he was not the person "behind the keyboard" for the subject hacks of Company A's network. In doing so, the government believes that King will try to pin the blame on St. Andria, who has been disclosed as a witness for the government and had an acrimonious falling out with King and his wife following a tripartite romantic relationship. As such, the government seeks to present evidence related to the 2004 Hack—including a recounting of King's admissions through the testimony of a special agent and King's father who were present when King was interviewed—for identification purposes and to demonstrate that King had the technical ability, and thus the opportunity, to accomplish the hacks subject of this proceeding.

Proof that King had the technical ability to accomplish the hacks subject of this proceeding provides evidence that identifies him, as opposed to St. Andria, as the person behind the computer hacks central to the allegations in the Superseding Indictment. See

⁶(...continued)

November 2015, the defendant and St. Andria allegedly used an account and password belonging to Company A employee Jerrord Qui to establish a virtual private network connection to Company A's computer network. *Id.* From there, they allegedly used an account and password belonging to Company A employee Francois Jacquot to begin navigating Company A's computer network. *Id.* After gaining access to Company A's computer network by impersonating these two employees, they purportedly increased Mr. Jacquot's account permissions and then installed three "hacking tools" onto Company A's computer network. *Id.*

During a search of his house in August 2016, the defendant admitted that he was familiar with the three "hacking tools" and that they were on a disc in his house. *Id.* Law enforcement recovered those same "hacking tools," among many others, on a disc in his house. *Id.* The defendant also admitted, among other things, that he was familiar with the fraudulent administrator accounts, had helped St. Andria with the scheme, and had forensically wiped St. Andria's work computer after Company A fired her. *Id.*

United States v. Barrett, 539 F.2d 244, 248 (1st Cir. 1976);⁷ see also *United States v. Zedner*, 401 F.3d 36, 49-50 (2d Cir. 2005), *rev'd on other grounds*, 547 U.S. 489 (2006).⁸

This technical ability also provides evidence of King's opportunity to commit the alleged crimes, which seemingly could not have been accomplished without such technical ability. See *United States v. Maravilla*, 907 F.2d 216, 222 (1st Cir.1990) ("To show 'opportunity' is to show that the defendant had some special capacity, ability or knowledge that would enable him to commit the crime."); *United States v. Green*, 648 F.2d 587, 592 (9th Cir.1981) ("Though the word ['opportunity' under 404(b)] has been little used by the courts it evidently is intended to cover all or a part of a category called 'capacity'")(citations omitted); see also *United States v. Slaughter*, 248 F. App'x 210, 212 (2d Cir. 2007)("Evidence showing that a defendant possessed a handgun prior to the charged crime is properly admitted to show access to such a weapon [under the opportunity exception to Rule 404(b)]."); *United States v. Robinson*, 560 F.2d 507, 513 (2d Cir.1977) (*en banc*) (finding that defendant's "possession of the gun was also admissible under [Rule 404(b)] on the independent ground that it tended to show he had the 'opportunity' to commit the bank robbery, since he had access to an instrument similar to that used to commit it"); *United States v. Scott*, 270 F.3d

⁷In *Barrett*, the defendant was accused of a burglary in which the burglars successfully bypassed a museum's alarm system. The defendant argued that he was misidentified by the government's witnesses. *Id.* at 247. On appeal, the First Circuit held that the district court properly admitted evidence of the defendant's "expertise with alarms" because it "indicated that [the defendant] had the skill to wire off the alarm system prior to the break-in and accordingly helped identify him as one of the guilty parties." *Id.* at 248.

⁸In *Zedner*, the defendant claimed the district court abused its discretion by admitting testimony of two rebuttal witnesses to the effect that Zedner committed frauds in 1988. The Second Circuit held that "[t]his evidence of fraud was offered for a proper purpose and was relevant. Zedner based his defense on the claim that he was delusional and lacked criminal intent because he did not know the bonds were counterfeit. Testimony about his other fraudulent acts tended to prove Zedner's financial sophistication, his ability to execute complex schemes, and his ability to form intent to defraud." *Id.* The Court also found that the probative value of the evidence outweighed any prejudice, and that the district court "reduced any risk of unfair prejudice with a carefully worded limiting instruction." *Id.*, at 50.

30, 47 (1st Cir. 2001) (“The evidence was relevant and admissible under Rule 404(b) because it showed [the defendant’s] opportunity to make withdrawals from the bank account, which linked him to the fraudulent tax returns.”), *cert. denied* 535 U.S. 1007 (2002); *United States v. Pouryan*, No. S1 11-CR-111 (NRB), 2013 WL 1348375, at *2 (S.D.N.Y. Apr. 4, 2013)(“In this case, evidence of the defendants’ alleged involvement in other international weapons transactions is admissible under Rule 404(b) to explain the development of the relationship between the co-conspirators and to demonstrate the defendants’ capacity, opportunity, and intent to provide weapons to the Taliban.”); *United States v. Tarantino*, No. 08-CR-655 JS, 2011 WL 1113504, at *5 (E.D.N.Y. Mar. 23, 2011) (Finding that testimony that the home invaders were armed and that they used stolen cars to carry out the crime was “Rule 404(b) ‘opportunity’ evidence admissible to show that the Defendant is guilty of the armored car robbery. . . . [E]vidence that [the Defendant] used a stolen car in the home invasion tends to show that he had the ability to steal cars. Each of these details is relevant because the Government anticipates that its witness will testify that the armored car robbers carried guns and fled the scene in a stolen vehicle. Accordingly, testimony that [the Defendant] and others were armed during the home invasion and that they used stolen cars is admissible under Rule 404(b).”). Thus, the evidence is offered for a proper purpose.

2. “relevant to a material issue in dispute”

Evidence that King demonstrated the technical ability to commit the crimes alleged here is relevant under Rule 401 because it has a tendency to make a fact that is of consequence in determining the instant action more or less probable. That is, it provides some evidence supporting the government’s theory that King either actually committed the

computer hacks, or instructed St. Andria on how to do so. Furthermore, the government has fulfilled its obligation to identify “a similarity or some connection between” the prior and current acts. *See United States v. Garcia*, 291 F.3d 127, 137 (2d Cir. 2002)(The government “must establish the relevance of the evidence to the issue in dispute. The government may not invoke Rule 404(b) and proceed to offer, carte blanche, any prior act of the defendant in the same category of crime. The government must identify a similarity or connection between the two acts that makes the prior act relevant to establishing knowledge of the current act.”). The fact that King was advised by an FBI agent that his conduct in 2004 violated federal law, however, is not probative of the purpose for which the evidence is being offered and therefore will not be allowed.

3. Rule 403

Although evidence may be relevant as directly probative of a defendant’s charged conduct, “this evidence may nonetheless be inadmissible pursuant to [Rule 403] if ‘its probative value is substantially outweighed by a danger of ... unfair prejudice.’” *United States v. Rivera*, No. 13-CR-149(KAM), 2015 WL 1875658, at *3 (E.D.N.Y. Apr. 22, 2015) (quoting Fed. R. Evid. 403, and citing *United States v. Bourne*, No. 08–CR–888, 2011 WL 4458846(NGG), at *12 (E.D.N.Y. Sept. 23, 2011)). “The term ‘unfair prejudice,’ as to a criminal defendant, speaks to the capacity of some concededly relevant evidence to lure the factfinder into declaring guilt on a ground different from proof specific to the offense charged.” *Old Chief v. United States*, 519 U.S. 172, 180 (1997). “In determining whether evidence is unfairly prejudicial, the court considers it in the context of the crime alleged, excluding evidence which is ‘more inflammatory than the charged crime.’” *United States v. Jefferys*, No. 18-CR-359(KAM), 2019 WL 5103822, at *10 (E.D.N.Y. Oct. 11, 2019) (quoting

United States v. Livoti, 196 F.3d 322, 326 (2d Cir. 1999)).

The fact that King hacked into his high school computer network when he was a high school sophomore and used techniques similar to those allegedly used here is not necessarily the type of evidence that would lure the factfinder into declaring guilt on a ground different from proof specific to the offenses for which he is charged. The evidence surrounding the 2004 Hack might support the government's theory that King had the technical ability to commit the crimes alleged. But this evidence is not more inflammatory, sensational, or disturbing than the crimes for which King is charged, and, therefore, is not unfairly prejudicial. See *United States v. Paulino*, 445 F.3d 211, 223 (2d Cir. 2006)(Probative value is not outweighed by prejudicial effect when the prior similar bad acts do not "involve conduct more inflammatory than the charged crime")(citation omitted); *United States v. Pitre*, 960 F.2d 1112, 1120 (2d Cir. 1992) (finding no unfair prejudice where "evidence of prior narcotics transactions 'did not involve conduct any more sensational or disturbing than the crimes with which [the appellants were] charged.'")(quoting *United States v. Roldan-Zapata*, 916 F.2d 795, 804 (2d Cir. 1990)). The Court finds that the probative value of evidence of the 2004 Hack that demonstrates that King had the technical ability to accomplish the crimes alleged here substantially outweighs any danger of unfair prejudice arising from it.

4. "limiting instruction"

To allow evidence from the 2004 Hack to be presented to the jury, the Court will require an appropriate limiting instruction to be given to the jury. Counsel for the parties are directed to confer in an attempt to reach a mutual agreeable limiting instruction.

5. Conclusion

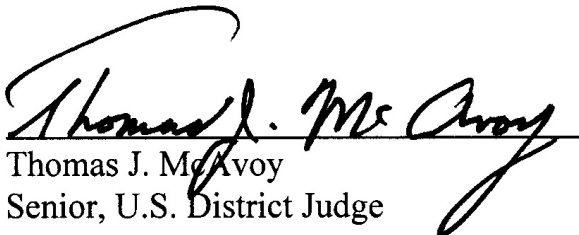
For the reasons discussed above, the government's in limine motion is granted to the extent it will be allowed to offer evidence from the 2004 Hack that demonstrates that King possessed the technical ability to accomplished the computer hacks subject of this case. To the extent King argues that this evidence is needlessly cumulative under Rule 403, that issue may be raised at trial.

III. CONCLUSION

For the reasons set forth above, Defendant King's omnibus pretrial motion, Dkt. No. 29, is **DENIED**. The government's motion in limine, Dkt. No. 46, is **GRANTED** as set forth herein.

IT IS SO ORDERED.

Dated: October 31, 2019


Thomas J. McAvoy
Senior, U.S. District Judge